# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/772,798 | 02/05/2004 | Jean-Philippe Wary | 704-011678-US (PAR) | 5205 |

2512 7590 05/15/2007

PERMAN & GREEN
425 POST ROAD
FAIRFIELD, CT 06824

| EXAMINER | |
|---|---|
| MEDE, ESTEVE | |
| **ART UNIT** | **PAPER NUMBER** |
| 2109 | |
| **MAIL DATE** | **DELIVERY MODE** |
| 05/15/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|  |  |  |
|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/772,798 | **Applicant(s)**<br>WARY, JEAN-PHILIPPE |
|  | **Examiner**<br>Esteve Mede | **Art Unit**<br>2109 |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *05 February 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *02/05/2004*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

### *Specification*

1. The disclosure is objected to because of the following informalities: in page 2, lines 7 the term "a person who does not known the key K" should be --a person who does not know the key k--; on page 6, lines 16 the term "sought co" should be --sought to--.

Appropriate correction is required.

### *Claim Objections*

2. Claims 1-10 are objected to because of the following informalities: in claim 1, line the term "the round functions" should be --round functions--; in claim 1, line 6 the term "the round functions" should be --round functions--; in claim 1, line 7-8 the term "by the conversion of digit words" should be --by a conversion of digit words--; in claim 1, line 9 the term "applied to these binary words" should be --applied to the binary words--; in claim 1, line 12 the "." (Period at the end of binary words) should be removed; in claims 2-10, lines 1 the term "a method" should be --the method--. Appropriate correction is required.

### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-2 are rejected under 35 U.S.C. 102(b) as being unpatentable by Adams et al. (5,949,884).

Regarding claim 1 Adams discloses a method wherein for the generation of a pseudo-random permutation of an N-digit word in which: a generalized Feistel scheme is implemented are functions (Fi) such that: an input words of the round functions are produced by the conversion of digit words into binary words (the limitation of a digit word converted into a binary word is inherent in the claimed invention as all data entered into an electronic device is automatically converted into binary); then a one-way function is applied to the binary words (see abstract, line 7); finally, the output in digits is a function of these binary words (the limitation of the output in digits is a function of these binary words an intrinsic property of the claimed invention as in a computing system when a digit is taking as input, it is converted to binary word as binary word is machine language all functions then take place on the binary word),and digit is giving at output digit word to be enciphered is read in a memory (the limitation of the digit word is read into memory is well known in the art is an intrinsic property of the invention as it is factual that all data in a computer system must first be read before it is encrypted); the generalized Feistel scheme used comprises at least T = 5 rounds (col. 3, lines 66-67).

Regarding claim 2, Adams discloses the method wherein the one-way function of the binary words users a standard pseudo-random cryptography function on binary words (col. 4, lines 16-17).

Regarding claim 3, Adams disclosed the method wherein the standard pseudo-random function on the binary words uses SHA-1 function (col. 2, lines 64-66).

Regarding claim 4, Adams discloses the method wherein the number of rounds T of the Feistel scheme is smaller than or equal to 30 (col. 3, lines 66-67).

## *Claim Rejections - 35 USC § 103*

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Adams et al. (US 5,949,884).

Regarding claim 5, Adams discloses all the limitation of claim 5, except that the rounds of the Feistel scheme are equal to six. The general concept of having the Feistel scheme rounds equal to 6 is well known in the art as illustrated by Adams, which discloses a Feistel scheme of 8 rounds (col. 3, lines 66-67). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Adams to include the use of 6 round Feistel scheme in order to provide suitable encryption on data.

7. Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adams et al. (US 5,949,884) in view of Coppersmith et al. (6,189,0095).

Regarding claim 6, Adams discloses all the limitation of claim 6 except that the method wherein during odd-value rounds of the Feistel scheme, the round function works on a word which a length B, and during even-valued rounds of the Feistel scheme it works on words within a length of A digits, where A+B = N. The general concept of during odd-valued the round function works on length B and during even-valued the round function works on length A is well known in the art as illustrated by Coppersmith, which discloses a Feistel scheme during odd-valued the function works on length S and during even valued works on length T where A+B = N (col. 3, lines30-41). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Adams to include the use of Coppersmith in order to apply the Feistel scheme on odd and even valued.

Regarding claims 8-10, Adams discloses all the limitation of claims 8-10, however Adams did not say that the length is between [7, 30], [10, 30] and [13, 30]. The general concept of having a predetermined length is well known in the art as illustrated by Coppersmith, which discloses a method of encrypting and decrypting an input message block of binary data of predetermined length (see abstract, lines 1-2). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Adams to include the used of predetermined input in order to specified the length of the inputs.

***Conclusion***

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Esteve Mede whose telephone number is 571-270-1594. The examiner can normally be reached on Monday thru Friday, 8:30-5:00 PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Jules can be reached on 571-272-6681. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Esteve Mede
em
May 4, 2007

FRANTZ JULES
SUPERVISORY PATENT EXAMINER